INTERIM STATEWIDE INFORMATION TECHNOLOGY STANDARD

Interim Standard: User Rights

Effective Date: May 30, 2007

Approved: Richard B. Clark

I. Standard Purpose

This interim standard defines the requirements for assigning user rights to those using workstations connected to the state's SummitNet network. It applies to all workstation users that connect to the state's SummitNet network.

This is an interim standard and may be reviewed upon publication of a security architecture but not later than one year from approval.

II. Background

The most common user rights configuration in the state environment is administrator level rights on workstations. Administrator level rights allow users to install and download software at the workstation level. This creates a security vulnerability that malware, worms and other attacks can exploit. In addition, administrator rights also mean that software downloads and installations are not being managed by agency information technology (IT) staff. This creates added overhead for user support, software patching, disaster recovery, desktop configuration and licensing.

Limiting user rights to workstations will help secure the network and make central administration of workstations easier for agency staff.

III. Definitions

<u>Standards:</u> Standards define the requirements or specifications for acceptable software, hardware, database, technical approach, business process, or methodology and must be complied with. All exceptions and changes must be documented, reviewed and approved.

<u>Standard User Account:</u> A minimal set of rights provided by the workstation operating system. This level of rights allows the employee to use most capabilities of the computer, but prevents the user from making changes to the operating system that impact other users of the workstation or the security of the workstation. These rights are at the workstation level.

<u>Local Administrator Account:</u> An advanced set of rights provided by the workstation operating system. This level of rights allows the employee to use all the capabilities of the computer, and allows the user to make changes to the operating system that impact other users of the workstation and the security of

the workstation. These rights are at the workstation level and should be assigned sparingly.

Network Administrator Account: A sophisticated set of rights provided by the network operating system. This level of rights is given to employees whose primary job duties are to administer workstations that are connected to the State of Montana network. These rights exist at a level beyond the workstation and allow a Network Administrator to make any change to any machine within his or her delegated authority.

User Rights: The permissions granted to access and use resources and information.

IV. Roles and Responsibilities

LAN Administrator, System Administrator: Some agencies may identify this role as LAN Manager, Network Administrator, Network Analyst or others. This role is typically given a network administrator account.

Agency Security Officer: This role typically performs a variety of tasks related to the security of information, establishment of user access rights and implementation of security policies and practices. Agency security officers will report as required to the State CIO on compliance with this standard.

V. Standard Requirements

A. Users will be assigned to the most restrictive type of account as defined in Section II that allows them to perform their job functions.

- Before assigning a user a local administrator account, application testing must be conducted to determine if assigning additional minimal rights will enable the application to run properly with a standard user account.

B. Each agency will be responsible for complying with this standard.

A semi-annual report will be submitted to the State CIO to provide a summary of user rights status. The report will show:

- The total number of users connecting to the network, including on-site contractors
- The total number of standard user accounts
- The total number of local administrator level accounts
  - If local administrator accounts are used, a general explanation and a brief migration strategy will be provided in the report
- The total number of network administrator level accounts

VI. Compliance Criteria

- Reports are accurate.
- Migration strategies are genuine attempts to move to standard user accounts.
- Agencies demonstrating that 100% of their users (with the exception of network administrators) are defined as standard user accounts will have the reporting requirement waived. An audit may be conducted periodically.

VII. Approved Product

Agencies may use the tool of their choice to measure compliance with this standard and to provide the required reporting.

Some solutions will be available from the Information Technology Services Division (ITSD) if desired. Contact the ITSD Service Desk (at http://servicedesk.mt.gov/ess.do) or at 444-2000 for assistance.

VIII. Support

Agencies will comply with this standard using the methods and tools appropriate for their individual agency. Testing documentation, forms, and tools are available and may be used for this purpose.

ITSD offers consultation at no charge to agencies experiencing difficulty complying with this standard. Consultation may include identifying options for applications not working properly with standard user accounts, providing a script for collecting compliance data or advising on other tools for compliance. In order to receive assistance, application testing results will be required. Free consultation does not include managing agency workstations or generating compliance reports unless a contract is in place for LAN services.

IX. Technical and Implementation Considerations

The shift to standard user accounts represents a major change in the way many agencies manage their users. There will be a considerable learning curve as the shift is made. It will mean a stronger reliance on information technology staff to manage user access and applications. It will also mean a more secure environment for all entities connecting to the state network. It is highly recommended that agencies be conscientious in their testing of applications and the application of standard user accounts. A serious effort must be undertaken to limit the number of users with local administrator accounts.

X. Change Control and Exceptions

Standard changes or exceptions are governed by the Procedure for Establishing and Implementing Statewide Information Technology Policies and Standards.

Requests for a review or change to this instrument are made by submitting an Action Request form (at http://itsd.mt.gov/policy/policies/action_request.doc). Requests for exceptions are made by submitting an Exception Request form (at http://itsd.mt.gov/policy/policies/exception_request.doc). Changes to policies and standards will be prioritized and acted upon based on impact and need.

XI. Closing

For questions or comments about this instrument, contact the State of Montana Chief Information Officer at ITSD Service Desk (at http://servicedesk.mt.gov/ess.do), or:

PO Box 200113
Helena, MT 59620-0113
(406) 444-2700
FAX: (406) 444-2701

XII. Cross-Reference Guide

For more information on the importance of limiting user rights, see:

- National Institute of Standards and Technology

A. State and Federal Laws

- 2-17-512, MCA. **Powers and duties of department.** The department [of Administration] (e) shall establish and enforce statewide information technology policies and standards
- 2-17-534, MCA. **Security responsibilities of department.** The department [of Administration] is responsible for providing centralized management and coordination of state policies for security of data and information technology resources
- 2-15-114, MCA. **Security responsibilities of departments for data.** Each department head is responsible for ensuring an adequate level of security for all data within that department and shall:
  (2) designate an information security manager to administer the department's security program for data

B. State Policies (IT Policies, MOM Policies, ARM Policies)

- ENT-SEC-112 – Workstation, Portable Computer and PDA (Personal Digital Assistant) Security
- ENT-SEC-063 – Usernames and Passwords

XIII. Administrative Use

History Log	
Deliverable ID:	STND-20070727a
Version:	1.0
Approved Date:	March 27, 2007
Effective Date:	May 30, 2007
Change & Review Contact:	ITSD Service Desk (at http://servicedesk.mt.gov/ess.do)
Review:	Event Review: Any event affecting this policy may initiate a review. Such events may include a change in statute, key staff changes or a request for review or change.
Scheduled Review Date:	1 year after Approved Date.
Last Review/Revision:	
Changes:	